

Safaricom Telecommunications Ethiopia PLC Anti-Money Laundering Policy Statement

Safaricom Telecommunications Ethiopia PLC and its subsidiaries (collectively “Safaricom”) are committed to complying with all applicable laws and regulations that are binding on Safaricom in the jurisdictions in which we operate, including laws relating to money laundering and terrorism financing.

Safaricom has therefore established a risk-based anti-money laundering (“AML”) and Countering the Financing of Terrorism (CFT) Policy and Program (“AML Program”).

The objective of the AML Program is to ensure that money laundering, terrorism financing and other financial crimes risks identified by Safaricom are appropriately addressed and mitigated. This is achieved by establishing policies that define the minimum standards, governing policies, principles, and controls which Safaricom must comply with.

The aim of our AML Program is to protect Safaricom, its employees, shareholders, customers, suppliers, vendors, business partners and third parties including the communities we serve from money laundering, terrorism financing and other financial crimes.

The AML Program includes but is not limited to:

1. Appointment of the Money Laundering Reporting Officer (MLRO) - The MLRO has been designated by Safaricom’s Board of Directors as the officer responsible for overseeing Safaricom AML Program, including appraising the Board of Directors and senior management of AML compliance initiatives, any significant compliance deficiencies, and the reporting of suspicious activity
2. Policies, procedures, and system of internal controls designed to facilitate ongoing compliance with applicable AML laws and regulations
3. Customer due diligence framework, which incorporates customer identification and verification including know your customer principles
4. Risk-based approach to AML monitoring and enhanced due diligence on customers assessed as higher risk, including PEPs and their relatives and close associates
5. Monitoring and reporting of suspicious activity to appropriate regulatory authorities
6. Mandated regular, independent testing and regular AML training
7. Record keeping requirements in accordance with applicable laws and regulations.

Execution of Safaricom’s AML Program is based on three lines of defense:

First Line of Defense - Each of Safaricom’s Businesses Units owns and manages the risks inherent in or arising from the business and is responsible for having controls in place to mitigate key risks, performing assessments of internal controls, and promoting a culture of compliance and control.

Second Line of Defense - Compliance provides support, oversight and set standards in accordance with applicable laws, codes, and generally acceptable management standards. We also provide ongoing advice and training to the business units and establish tools, methodologies, processes, and controls used by the business units to foster a culture of compliance. The AML team is responsible for coordinating, monitoring, and overseeing day-to-day compliance with the AML Program.

Third Line of Defense – Safaricom’s Internal Audit function independently reviews activities of the first two lines of defense based on a risk-based audit plan and methodology approved by the Safaricom Board of Directors.

Safaricom may revise its AML policy from time to time as and when necessary to ensure internal compliance measures remain current and effective. Policies and controls will continually be developed and reviewed to ensure that money laundering, terrorist financing and other financial crimes risks are managed in accordance with appropriate regulatory and industry standards.